What is claimed is:

1. A system for verifying the availability of a back-up secure tunnel between a pair of network elements in a communications network, comprising:

a first network element for originating and transmitting a back-up tunnel verification test message to a second network element using the back-up secure tunnel in response to the receipt of a back-up tunnel verification test command;

a second network element for receiving the backup tunnel verification test message and transmitting a response back to the first network element using the back-up secure tunnel; and

a backup tunnel verification function logic module in the first network element for accumulating a number of failures to respond by the second network element to the backup tunnel verification tests performed during an active verification period and determining if the accumulated number of failures is less than a threshold value specified in the backup tunnel verification test command.

2. The system for verifying the availability of a back-up secure tunnel of claim 1 wherein the backup tunnel verification function logic module further determines the number of successful responses to the back up tunnel verification tests performed.

3. The system for verifying the availability of a back-up secure tunnel of claim 1 further comprising a computer connected to the communications network and running a network management application that transmits the backup tunnel verification test command to the first network element.

4. The system for verifying the availability of a back-up secure tunnel of claim 1 further comprising a console interface on the first network element for generating the backup tunnel verification test command.

5. The system for verifying the availability of a back-up secure tunnel of claim 1 wherein the back-up tunnel verification function is initiated by a configuration of a network element that forms an endpoint of the back-up secure tunnel.

6. The system for verifying the availability of a back-up secure tunnel of claim 1 further comprising two unidirectional tunnels that form the back-up secure tunnel.

7. The system for verifying the availability of a back-up secure tunnel of claim 1 wherein the communications network is a virtual private network (VPN).

8. The system for verifying the availability of a back-up secure tunnel of claim 1 wherein the back-up secure tunnel is an Internet Protocol Security (IPSec) tunnel.

9. The system for verifying the availability of a back-up secure tunnel of claim 8 wherein the back-up tunnel verification test message is an IPSec tunnel ping.

10. The system for verifying the availability of a back-up secure tunnel of claim 1 further comprising a primary secure tunnel for handling data traffic between the pair of network elements.

11. The system for verifying the availability of a back-up secure tunnel of claim 1 wherein the backup tunnel verification test command includes an identification of the secure tunnel to test, and a time interval during which a number of backup tunnel verification tests are performed.

12. The system for verifying the availability of a back-up secure tunnel of claim 11 wherein the backup tunnel verification test command further comprises a time to wait between each backup tunnel verification test and a payload size of a backup tunnel verification test packet.

13. The system for verifying the availability of a back-up secure tunnel of claim 6 wherein a first back-up unidirectional tunnel is used to send an Internet Protocol Security (IPSec) tunnel ping from the first network element to the second network element, and a second back-up unidirectional tunnel is used to send a response IPSec tunnel ping from the second network element to the first network element.

14. The system for verifying the availability of a back-up secure tunnel of claim 1 further comprising a plurality of back-up secure tunnels between the pair of network elements.

15. A method for verifying the availability of a back-up secure tunnel between a pair of network elements in a communications network, comprising the acts of:

originating and transmitting a backup tunnel verification test message from a first network element to a second network element using the back-up secure tunnel in response to the receipt of a backup tunnel verification test command;

receiving the backup tunnel verification test message from a second network element and transmitting a response back to the first network element using the back-up secure tunnel; and

accumulating a number of failures to respond by the second network element to the backup tunnel verification tests performed during an active verification

period and determining if the accumulated number of failures is less than a threshold value specified in the backup tunnel verification test command.

16. The method for verifying the availability of a back-up secure tunnel of claim 15 further comprising determining the number of successful responses to the backup tunnel verification test.

17. The method for verifying the availability of a back-up secure tunnel of claim 15 further comprising transmitting the backup tunnel verification test command from a network management application to the first network element.

18. The method for verifying the availability of a back-up secure tunnel of claim 15 further comprising generating the backup tunnel verification test command at a console interface on the first network element.

19. The method for verifying the availability of a back-up secure tunnel of claim 15 further comprising initiating a back-up tunnel verification function by an initial configuration of a network element that forms an endpoint of the back-up secure tunnel.

20. The method for verifying the availability of a back-up secure tunnel of claim 15 wherein the back-up secure tunnel is formed from two unidirectional tunnels.

21. The method for verifying the availability of a back-up secure tunnel of claim 15 wherein the communications network is a virtual private network (VPN).

22. The method for verifying the availability of a back-up secure tunnel of claim 15 wherein the back-up secure tunnel is an Internet Protocol Security (IPSec) tunnel.

23. The method for verifying the availability of a back-up secure tunnel of claim 22 wherein the backup tunnel verification test message is an IPSec tunnel ping.

24. The method for verifying the availability of a back-up secure tunnel of claim 15 wherein the backup tunnel verification test command includes an identification of the back-up secure tunnel to test, and a time interval during which a number of backup tunnel verification tests are performed.

25. The method for verifying the availability of a back-up secure tunnel of claim 24 wherein the backup tunnel verification test command further comprises a time to wait between each backup tunnel verification test and a payload size of a backup tunnel verification test packet.

26. The method for verifying the availability of a back-up secure tunnel of claim 20 wherein a first unidirectional tunnel is used to send an Internet Protocol Security (IPSec) tunnel ping from the first network element to the second network element, and a second unidirectional tunnel is used to send a response IPSec tunnel ping from the second network element to the first network element.

27. A computer readable medium containing a computer program product for verifying the availability of a back-up secure tunnel between a pair of network elements in a communications network, the computer program product comprising:

program instructions that originate and transmit a backup tunnel verification test message to a paired network element using the back-up secure tunnel in response to the receipt of a backup tunnel verification test command;

program instructions that receive a backup tunnel verification test message and transmit a response back to a paired network element using the back-up secure tunnel; and

program instructions that accumulate a number of failures to respond by the second network element to the backup tunnel verification tests performed during an active verification period and determine if the accumulated number of

failures is less than a threshold value specified in the backup tunnel verification test command.

28. The computer program product for verifying the availability of a back-up secure tunnel of claim 27 further comprising program instructions that determine the number of successful responses to the backup tunnel verification tests performed.

29. The computer program product for verifying the availability of a back-up secure tunnel of claim 27 further comprising program instructions that receive the backup tunnel verification test command from a network management application.

30. The computer program product for verifying the availability of a back-up secure tunnel of claim 27 further comprising program instructions that generate the backup tunnel verification test command.

31. The computer program product for verifying the availability of a back-up secure tunnel of claim 27 wherein two unidirectional tunnels form the back-up secure tunnel.

32. The computer program product for verifying the availability of a back-up secure tunnel of claim 27 wherein the back-up secure tunnel is an Internet Protocol Security (IPSec) tunnel.

33. The computer program product for verifying the availability of a back-up secure tunnel of claim 27 wherein the communications network is a virtual private network (VPN).

34. The computer program product for verifying the availability of a back-up secure tunnel of claim 32 wherein the back-up tunnel verification test message is an IPSec tunnel ping.

35. The computer program product for verifying the availability of a back-up secure tunnel of claim 27 wherein the backup tunnel verification test command includes an identification of the secure tunnel to test, and a time interval during which a number of back-up tunnel verification tests are performed.

36. The computer program product for verifying the availability of a back-up secure tunnel of claim 35 wherein the backup tunnel verification test command further comprises a time to wait between each back-up tunnel verification test and a payload size of a back-up tunnel verification test packet.

37. The computer program product for verifying the availability of a back-up secure tunnel of claim 31 wherein a first unidirectional tunnel is used to send an Internet Protocol Security (IPSec) tunnel ping from the first network element to the second network element, and a

second unidirectional tunnel is used to send a response IPSec tunnel ping from the second network element to the first network element.

38. A method for determining the identity of a back-up secure tunnel between a pair of network elements in a communications network, comprising the acts of:

obtaining a back-up tunnel policy name using a pointer to a back-up tunnel policy from a primary tunnel policy stored at a first network element;

determining if the back-up secure tunnel is an Internet Key Exchange (IKE) tunnel;

if the back-up secure tunnel is an IKE tunnel, determining if an IKE phase II connection between the pair of network elements has been established;

requesting an IKE phase I connection to generate an IKE phase II connection if it has not been established previously;

generating the back-up tunnel identification when the IKE phase II connection has been established.

39. The method for determining the identify of a back-up secure tunnel of claim 38 wherein the back-up secure tunnel is formed from two unidirectional tunnels.

40. The method for determining the identify of a back-up secure tunnel of claim 38 wherein the communications network is a virtual private network (VPN).

41. The method for determining the identify of a back-up secure tunnel of claim 38 wherein the back-up secure tunnel is an Internet Protocol Security (IPSec) tunnel.

42. A method for determining the identity of a back-up secure tunnel between a pair of network elements in a communications network, comprising the acts of:

obtaining a back-up tunnel policy name using a pointer to a back-up tunnel policy from a primary tunnel policy stored at a first network element;

determining if the back-up secure tunnel is a manually generated tunnel;

generating the back-up tunnel identification if the back-up secure tunnel is a manually generated tunnel.

43. The method for determining the identify of a back-up secure tunnel of claim 42 wherein the back-up secure tunnel is formed from two unidirectional tunnels.

44. The method for determining the identify of a back-up secure tunnel of claim 42 wherein the communications network is a virtual private network (VPN).

45. The method for determining the identify of a back-up secure tunnel of claim 42 wherein the back-up secure tunnel is an Internet Protocol Security (IPSec) tunnel.